*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

07/23/2014

**SUBJECT:**

Multiple Vulnerabilities in Mozilla Firefox and Thunderbird Could Allow for Remote Code Execution

**EXECUTIVE SUMMARY:**

Multiple vulnerabilities have been identified in Mozilla Firefox and Thunderbird which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet and Mozilla Thunderbird is an email client. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Mozilla Firefox versions prior to 31
- Mozilla Firefox Extended Support Release (ESR) version prior to 24.7
- Mozilla Thunderbird versions prior to 31

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High**

**TECHNICAL SUMMARY:**

Fourteen vulnerabilities have been reported in Mozilla Firefox and Thunderbird. Details of the vulnerabilities are as follows:

- A security bypass vulnerability exists because the applications fail to properly enforce the same-origin policy. An attacker can use ‘frame’ tags to bypass same-origin policy and execute arbitrary script code in the context of another domain. [CVE-2014-1552, MFSA 2014-66]
- Three vulnerabilities exist due to a failure to parse SSL certificates that use non-standard character encoding. Use of nonstandard characters in a certificate can cause a potential inability to use valid SSL certificates. [CVE-2014-1558, CVE-2014-1559, CVE-2014-1560, MFSA 2014-65]
- A vulnerability exists in the Skia library when scaling high quality images. If image scaling takes too long, a crash occurs causing image data to be discarded while still in use by the scaling operation. [CVE-2014-1557, MFSA 2014-64]
- A use after free vulnerability exists while manipulating certificates in the trusted cache. A crash can be caused as a result of a pair of NSSCertificate structures being added to a trust domain and then one of them is removed while they are still in use by the trusted cache. [CVE-2014-1544, MFSA 2014-63]
- A remote code execution vulnerability exists in these applications when using the Cesium JavaScript library to generate WebGL content. [CVE-2014-1556, MFSA 2014-62]
- A use after free vulnerability exists when the FireOnStateChange event is triggered in certain ciscumstances. [CVE-2014-1555, MFSA 2014-61]
- A vulnerability exists that allows for event spoofing attacks. It is possible to create a drag and drop event in web content which mimics the behavior of a chrome customization event. This can occur when a user is customizing a page or panel. This results in a limited ability to move UI icons within the visible window but does not otherwise affect customization or window content. [CVE-2014-1561, MFSA 2014-60]
- A use after free vulnerability exists due to an error in how font resources and tables are handled when rendering MathML content with DirectWrite fonts. [CVE-2014-1551, MFSA 2014-59]
- A heap use after free memory corruption vulnerability exists in Web Audio due to incorrect control message ordering. [CVE-2014-1550, MFSA 2014-58]
- A remote heap based buffer overflow vulnerability occurs during Web Audio buffering for playback. This occurs because of an error in the amount of allocated memory for buffers. This leads to a potentially exploitable crash with some audio content. [CVE-2014-1549, MFSA 2014-57]
- Two memory corruption vulnerabilities exist in affected versions of Mozilla Firefox. Mozilla developers and community identified and fixed several memory safety bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these bugs showed evidence of memory corruption under certain circumstances, and we presume that with enough effort at least some of these could be exploited to run arbitrary code. [CVE-2014-1547, CVE-2014-1548, MFSA 2014-56]

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Mozilla to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

**REFERENCES:**

**Mozilla:**

https://www.mozilla.org/security/announce/

https://www.mozilla.org/security/announce/2014/mfsa2014-66.html

https://www.mozilla.org/security/announce/2014/mfsa2014-65.html

https://www.mozilla.org/security/announce/2014/mfsa2014-64.html

https://www.mozilla.org/security/announce/2014/mfsa2014-63.html

https://www.mozilla.org/security/announce/2014/mfsa2014-62.html

https://www.mozilla.org/security/announce/2014/mfsa2014-61.html

https://www.mozilla.org/security/announce/2014/mfsa2014-60.html

https://www.mozilla.org/security/announce/2014/mfsa2014-59.html

https://www.mozilla.org/security/announce/2014/mfsa2014-58.html

https://www.mozilla.org/security/announce/2014/mfsa2014-57.html

https://www.mozilla.org/security/announce/2014/mfsa2014-56.html

**CVE:**

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1552

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1558

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1559

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1560

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1557

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1544

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1556

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1555

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1561

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1551

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1550

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1549

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1547

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1548

**Security Focus:**

http://www.securityfocus.com/bid/68810

http://www.securityfocus.com/bid/68811

http://www.securityfocus.com/bid/68812

http://www.securityfocus.com/bid/68813

http://www.securityfocus.com/bid/68814

http://www.securityfocus.com/bid/68815

http://www.securityfocus.com/bid/68816

http://www.securityfocus.com/bid/68817

http://www.securityfocus.com/bid/68818

http://www.securityfocus.com/bid/68820

http://www.securityfocus.com/bid/68821

http://www.securityfocus.com/bid/68822

http://www.securityfocus.com/bid/68824

http://www.securityfocus.com/bid/68826